Security through obfuscation

How state actors use proxies in cyber conflict

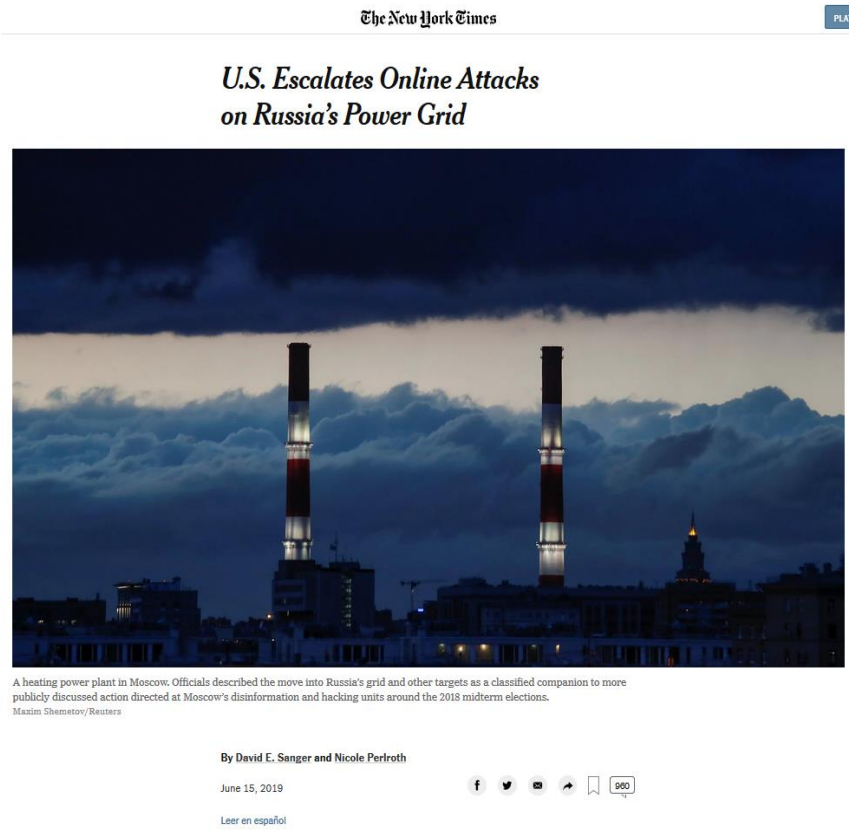
Vortrag zum Interdisziplinären Fakultätsseminar, Fakultät Wirtschafts- und Sozialwissenschaften,

Universität Heidelberg, 23.07.2019

DSF Deutsche Stiftung Friedensforschung
german foundation for peace research

Introduction

- Cyber-attacks conducted by states and their proxies receive more and more public/ scholarly attention.
- It appears that cyber-proxies carry out a significant part of political attacks, especially on behalf of autocratic regimes (Schmitt & Vihul, 2014).
- No study as of yet has empirically analyzed what kind of targets are attacked under what conditions by proxies and how these attacks differ from those conducted by state authorities
- Research questions:
  1. Which states are the most frequent users of proxies?
  2. Do attacks conducted by states and proxies follow different patterns?
  3. How do the most frequent state users employ proxies and do they differ in their operational deployment?



The New York Times

U.S. Escalates Online Attacks on Russia's Power Grid

A heating power plant in Moscow. Officials described the move into Russia's grid and other targets as a classified companion to more publicly discussed action directed at Moscow's disinformation and hacking units around the 2018 midterm elections.
Maxim Shemetov/Reuters

By David E. Sanger and Nicole Perlroth

June 15, 2019

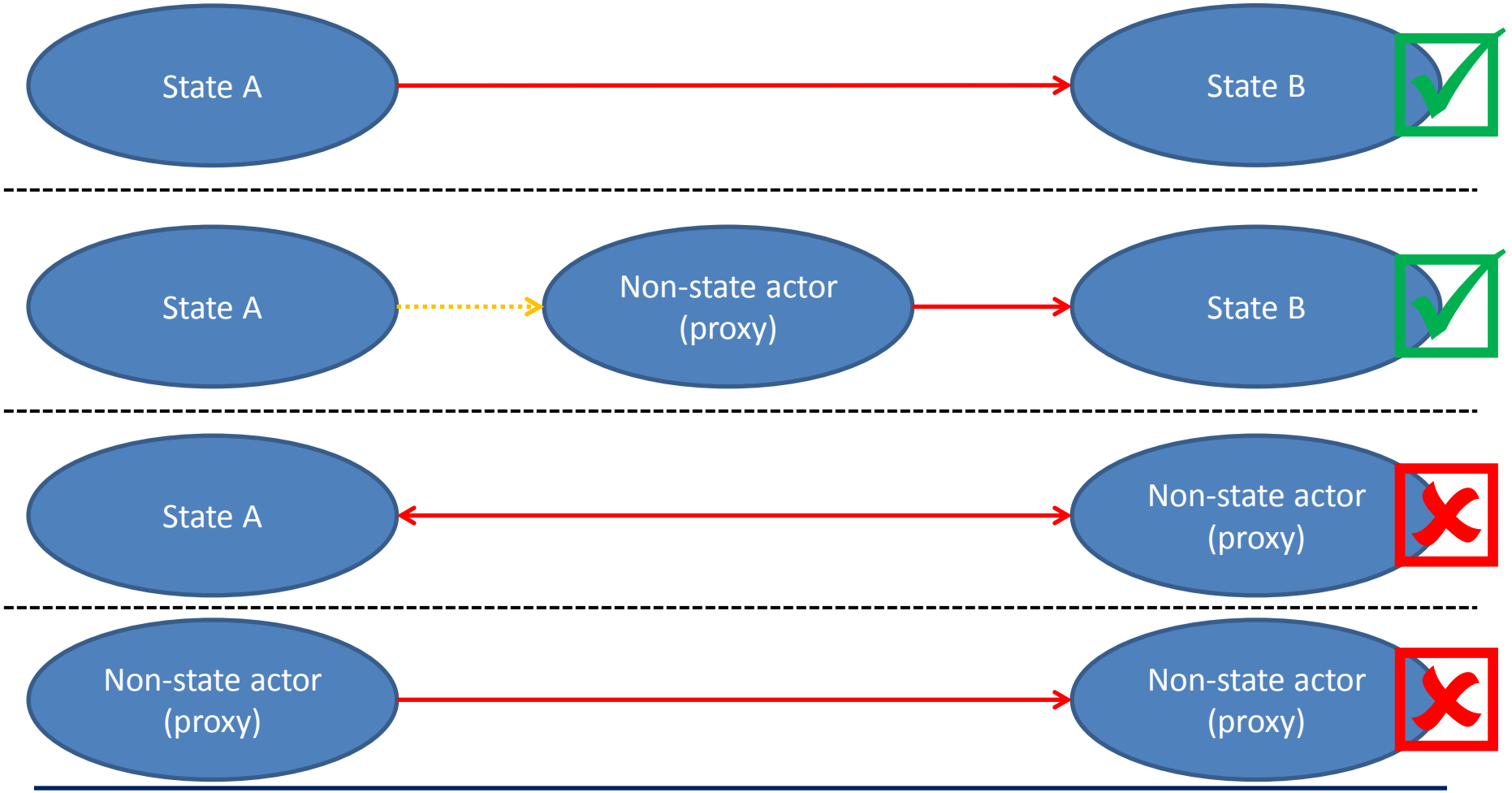
Leer en español

Current state of research

- Focus of literature is on prominent interstate incidents through single case studies
  - the attacks on Estonian internet infrastructures in 2007 (Herzog, 2011; Ottis, 2008; Tikk, Kaska, & Vihul, 2010),
  - Stuxnet (Farwell & Rohozinski, 2011; Jenkins, 2013; Lindsay, 2013; Zetter, 2014),
  - the Sony-Hack (Sharp, 2017; Shaw & Jenkins, 2017; Sullivan, 2016) or
  - the DNC-Hack (Jamieson, 2018; Lam, 2018).
- The few studies on state-proxy interaction foreground principal-agent relations (Bertram, 2017; Maurer, 2016, 2018a, 2018b).
- Valeriano and Maness established the first data set of cyber attacks conducted by states (2014, 2015).
- The Council on Foreign Relations launched the *Cyber Operations Tracker* with a focus on state-sponsored cyber-attacks in 2017 (CFR 2017).

The project

State of research: empirical gaps and deficits



Theoretical & methodological gaps and deficits

1. Current literature highlights incidents and not interaction patterns.
2. The attribution problem looms large: under what conditions do state actors shy away from attributing an attack?
3. There is no systematic integration of on- and offline conflict studies, i.e. the potential inaction patterns between both interaction levels
4. Thus far, the literature still faces deficits when conceptualizing measuring the intensity score of attacks, i.e. the gap between the physical/kinetic and political, economical effects.

Key concepts: definitions

- **Cyber-Conflict**

  "…a political conflict is a perceived incompatibility of intentions between individuals or social groups. Such an incompatibility emerges from the presence of actors who communicate and act with regard to certain objects. These actions and communications are known as measures, while the objects form the issues of positional differences. Actors, measures [in our case cyber attacks; SeH], and issues are the constitutive attributes of political conflict." (HIIK 2017)

- **Conceptualization of Cyber attack**

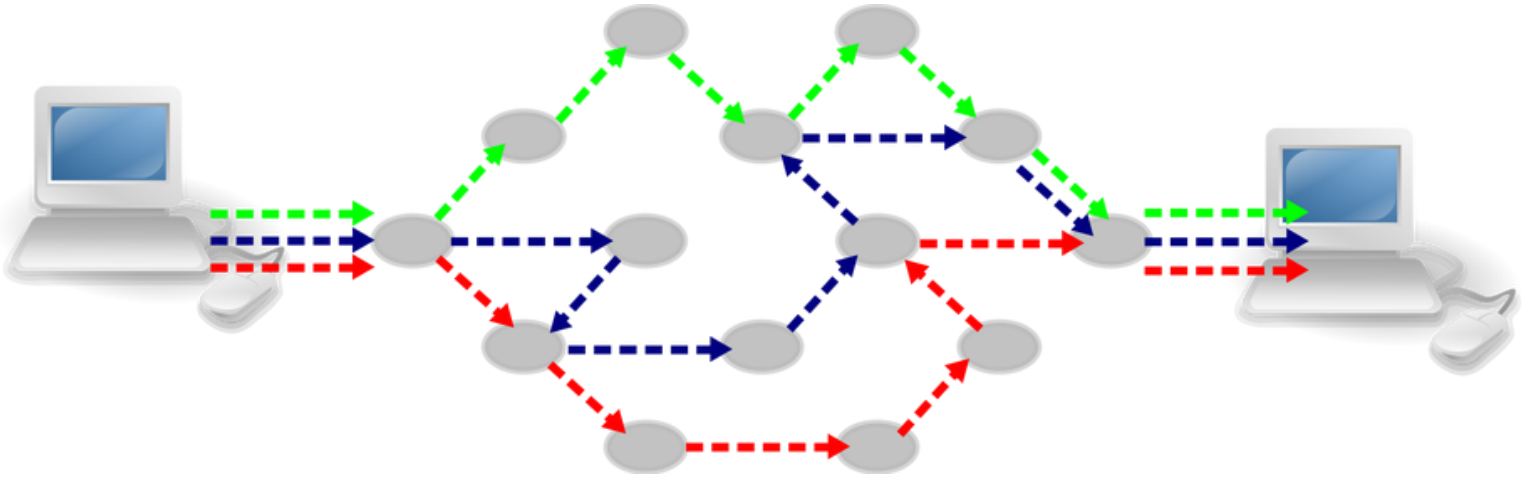
  willful and illegal act in the cyber space to compromise the condidentiality, integrity or availability of data (software) or cyber infrastructure (hardware) (so-called CIA Triade) (Oscarson 2003).

- **Cyber proxy**

  A cyber proxy is „an intermediary who carries out offensive and defensive measures with the knowledge or support of a beneficiary/client" (Maurer, 2018, p. 32).

The attribution problem: conceptualization

- „In the context of computer network intrusions, attribution is commonly seen as one of the most intractable technical problems...” (Rid 2014: 4)

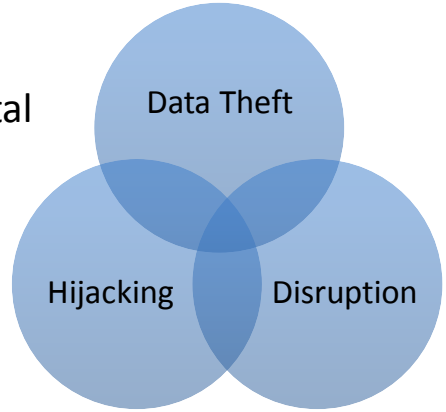


Paketvermittelte Kommunikation, Quelle: https://commons.wikimedia.org/wiki/File:CPT-internet-packetswitching.svg

- Attribution is based on a) claim of attacker; b) attribution of attacked (politicization); c) ascription of scientific/cyber security community.
- Plausibility probe whether attacker may have the technical expertise (i.e. access to Zero-Day-Exploits

Data and Methodology

- We draw on a sample of 197 cyber-attacks conducted by states or proxies between 2007 and 2016 (the sample is part of a HD-CYCon data set at Heidelberg University).
- *Attribution* of attacks is established by triangulating different sources, including the target, the attacker and the IT-security-community. Based on these information attacks are ascribed to either being conducted by a state or a proxy.
- Incidents are then assigned to categories, that mark *different modes of operation*: data theft, disruption, hijacking.
- To assess the *severity* of each incident, the impacts on- and offline are identified and scores of 0-2 are assigned in each category mentioned + physical effects are evaluated with regard to spatial and temporal dimensions. The theoretical maximum score is 15, because the score of attacks with far reaching societal effects are multiplied by 1.5.
- *Receiver-Categories*: State institutions/political system, International/ supranational organizations, Critical infrastructure, Social groups, Commercial entities, End user(s), Media, Science, Other.

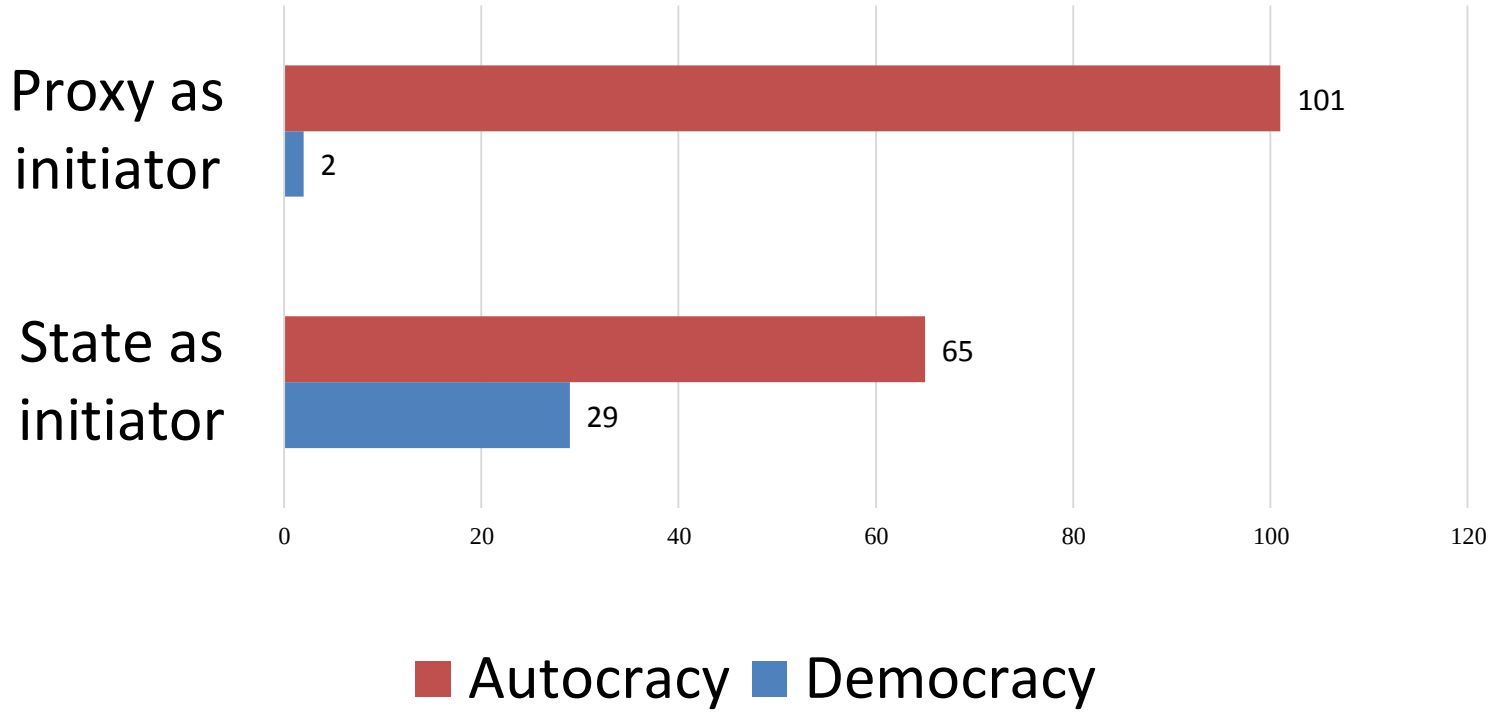


Preliminary findings

States and their cyber proxies

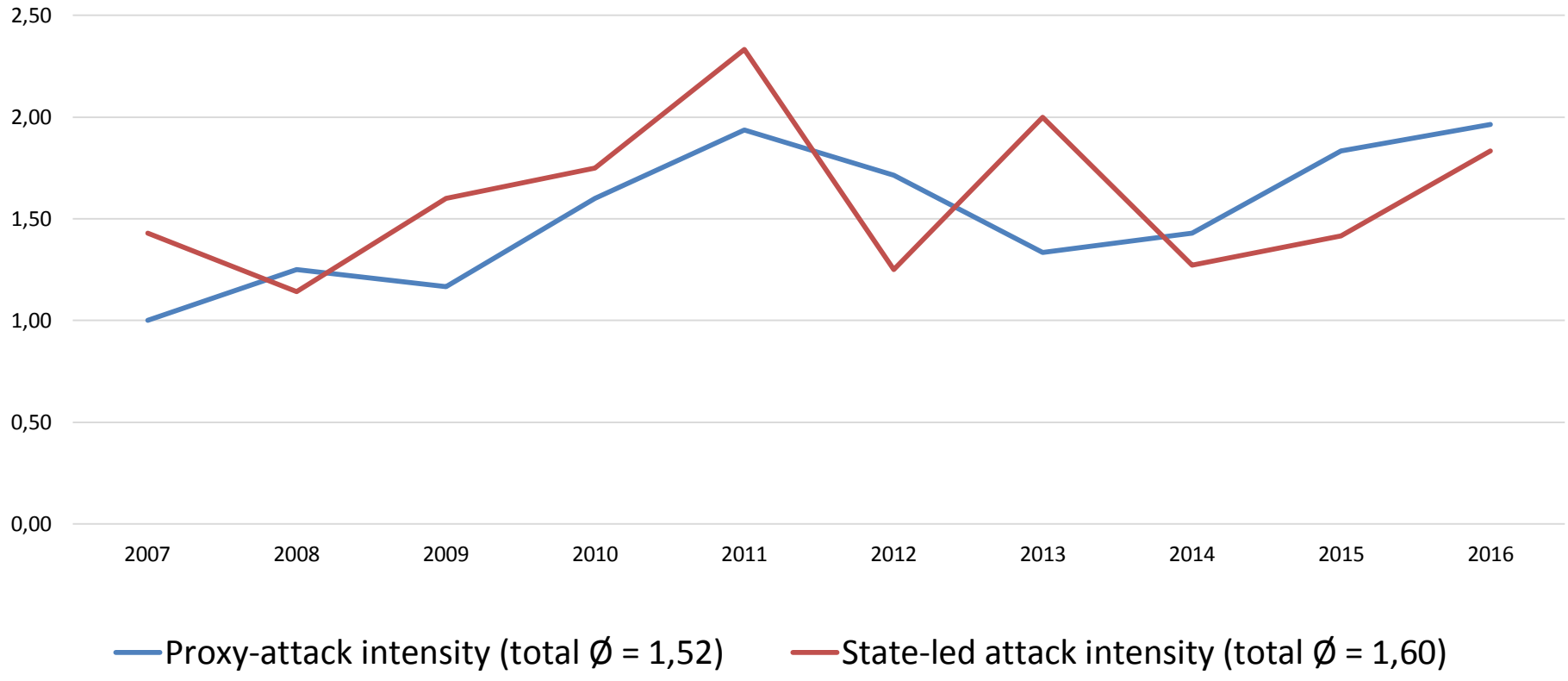
Findings I: Initiator Regime type

Autocracies as the far more active cyber-actors:



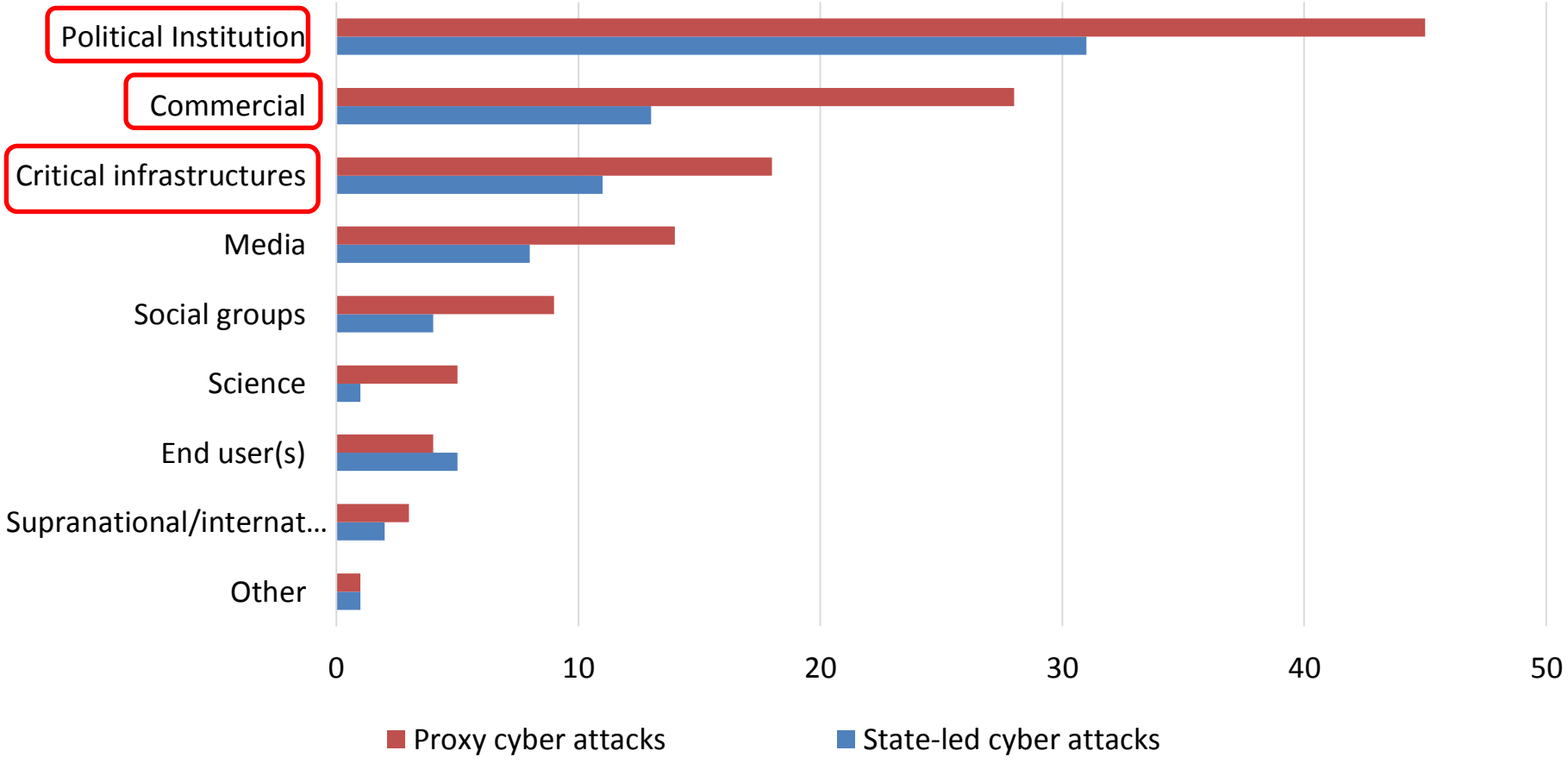
Findings II: Intensity scores

Relatively low average-intensity, for both attack-types:



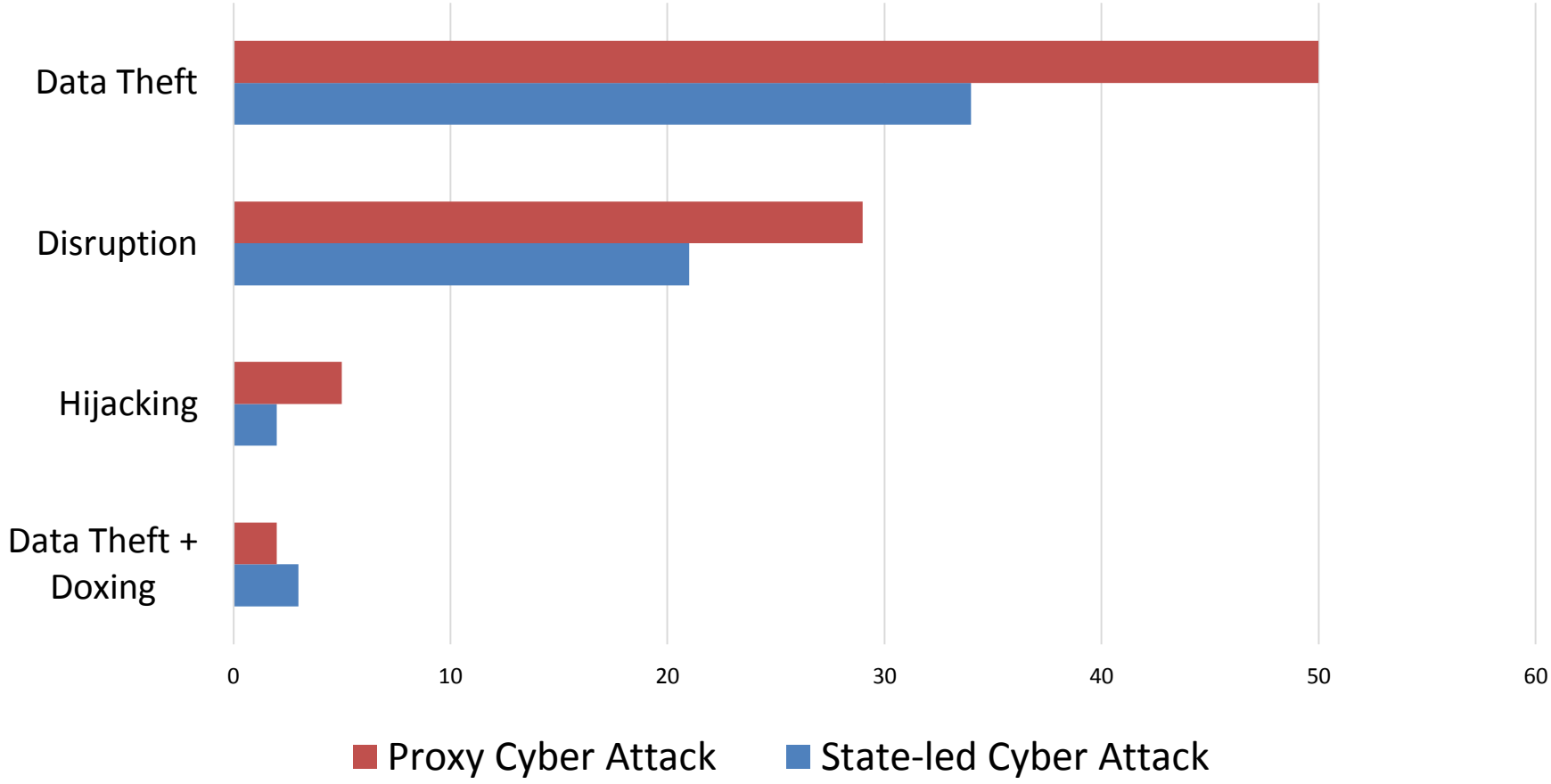
Findings III: Receiver Categories

Similar patterns for the respective receiver categories in both-attack types:



Findings IV: Types of incidents

Similar patterns for the respective incident types in both attack-categories:



Findings V: Top 4 proxy-using autocracies in comparison

	Proxy-attacks	State-led attacks
1. China CN	33	27
2. Syria S?	24	2
3. Iran IR	17	6
4. Russia RU	15	15

Proxy-attack total: 89
State-led-attack total: 50

Findings: China and Russia

China CN

- **Dominant:** data theft targetting commercial entities, political institutions and critical infrastructures
- Applies for state-led & proxy-attacks

➢ **Proxy-use embedded in overall economic agenda (5-years-plans)**

Russia RU

- **Proxies:** targetting political institutions and critical infrastructures (Ukraine)
- Both data theft & disruption
- **State-led:** targetting commercial entities rather than Critical Infrastr
- Data theft, disruption & doxing

➢ **Proxy-use embedded in overall geopolitical agenda, but with subtle differences**

Findings: Iran and Syria

Iran IR

- Proxy-attacks > state-led attacks
- **Proxies:** targetting commercial entities & politicial institutions, less CI
- **State-led attacks:** mostly targetting military-political sector
- **Both:** data theft & disruption

➢**Proxies: international agenda**

➢**State-led: regional/national agenda**

Syria S□

- Proxy-attacks >> state-led-attacks
- **Proxies**: targeting political targets, commercial entities and CI
- Data theft and/or disruption
- **State-led attacks:** vs. Media, Enduser and Commercial entities

➢**Proxies (esp. SEA) primarily aimed at (ideological) opponents**

➢**Spying against local adversaries of the regime**

Conclusion

1. General state-proxy interaction patterns across the different categories indicate proxies as an extension of autocratic cyber-strategies but of not offline security strategies
2. There are notable differences among the top 4 cyber-proxy using states:
    1. Russia and China used proxies indeed as an extension of their own state-capabilities
    2. Iran and Syria much more relied on proxies for offensive-cyber-actions
3. Plausible additional explanatory factors include the respective regional conflict environments (e.g. Syria-, Ukraine-wars), international rivalries (e.g. US vs. Iran) as well as economic goals (especially China)

Thank you for your attention

https://www.uni-heidelberg.de/fakultaeten/wiso/ipw/mitarbeiter/harnisch/

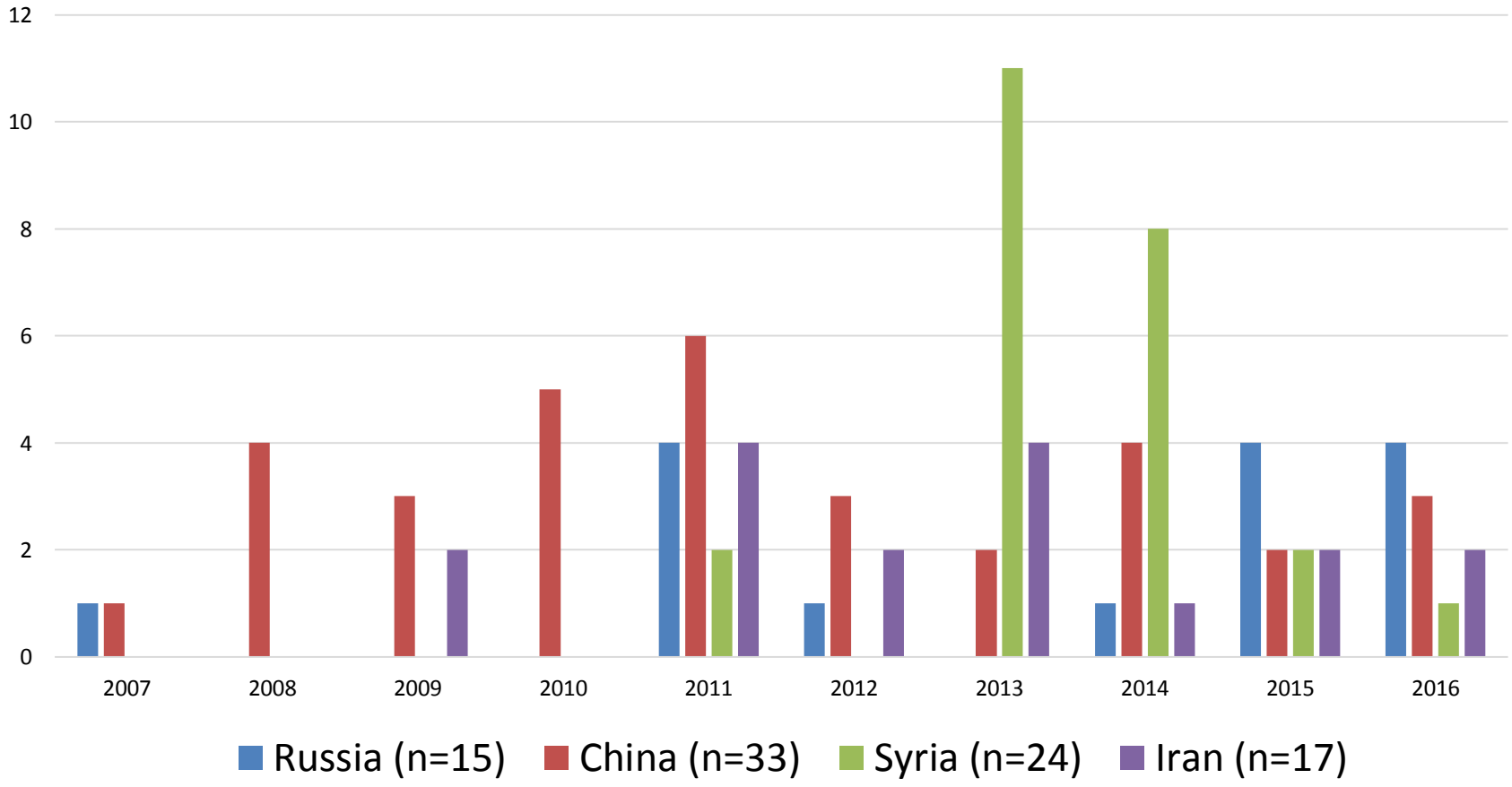
References (I)

- Bertram, S. K. (2017). Close enough – The link between the Syrian Electronic Army and the Bashar al-Assad regime. Journal of Terrorism Research, 8(1), 2–17. Retrieved from http://jtr.st-andrews.ac.uk/articles/10.15664/jtr.1294/galley/974/download/
- CFR 2017: Cyber Operations Tracker, in: https://www.cfr.org/interactive/cyber-operations [last accessed 20 November 2017].
- Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. Survival, 53(1), 23–40. https://doi.org/10.1080/00396338.2011.555586
- Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, 4(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3
- Jamieson, K. H. (2018). Cyberwar: How russia helped elect a President - What We Don't, Can't, and Do Know. New York: Oxford University Press.
- Jenkins, R. (2013). Is Stuxnet physical? Does it matter? Journal of Military Ethics, 12(1), 68–79. https://doi.org/10.1080/15027570.2013.782640
- Lam, C. (2018). A Slap on the Wrist:: Combatting Russia's Cyber Attack on the 2016 US Presidential Election. Boston College Law Review, 59(6), 2167–2201.
- Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122
- Maurer, T. (2016). 'Proxies' and Cyberspace. Journal of Conflict and Security Law, 21(3), 383–403. https://doi.org/10.1093/jcsl/krw015
- Maurer, T. (2018a). Cyber Mercenaries: The state, hackers, and power. Cambridge: Cambridge University Press.
- Maurer, T. (2018b). Cyber Proxies and Their Implications for Liberal Democracies. The Washington Quarterly, 41(2), 171–188. https://doi.org/10.1080/0163660X.2018.1485332
- Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. In D. Remenyi (Ed.), Proceedings of the 7th European Conference on Information Warfare and Security (pp. 163–168). Reading: Academic Publishing Limited.

References (II)

- Schmitt, M., & Vihul, L. (2014). Proxy Wars in Cyberspace. Fletcher Security Review, 1(2), 54–73.
- Sharp, T. (2017). Theorizing cyber coercion: The 2014 North Korean operation against Sony. Journal of Strategic Studies, 58(3), 1–29. https://doi.org/10.1080/01402390.2017.1307741
- Shaw, T., & Jenkins, T. (2017). An Act of War? The Interview Affair, the Sony Hack, and the Hollywood–Washington Power Nexus Today. Journal of American Studies, 29, 1–27. https://doi.org/10.1017/S0021875817000512
- Sullivan, C. (2016). The 2014 Sony Hack and the Role of International Law. Journal of National Security Law & Policy, 8(3).
- Tikk, E., Kaska, K., & Vihul, L. (2010). International Cyber Incidents: Legal Considerations. Retrieved from https://ccdcoe.org/publications/books/legalconsiderations.pdf
- Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. Journal of Peace Research, 51(3), 347–360. https://doi.org/10.1177/0022343313518940
- Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford, New York: Oxford University Press.
- United Nations. (2013). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Retrieved from https://undocs.org/A/68/98
- Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon (First edition). New York: Crown Publishers.

State-sponsored proxy-attacks by autocratic regimes (total: 89)



State-led cyber-attacks by autocratic regimes (total: 50)